SCRIPTING VIRUS SCAN ENGINE

ABSTRACT OF THE DISCLOSURE

Detecting and identifying an interpreted language virus, such as a scripting virus, and reasonably identifiable polymorphs of the virus source code. Scripting virus source is extracted and represented in a language independent form. This form includes a linearized set of key actions, termed an executing thread, rather than the scripting source code. The executing thread can be utilized to generate a virus signature and virus pattern file for use in identifying the virus in later extracted scripting virus source code. Further the executing thread may be compared to existing virus signatures to determine the identity of the virus, if a match is made. The scripting virus scan engine detects reasonably identifiable polymorphs of a scripting virus source code that involve lexical and grammatical transformations, such as manipulation of white space, renaming of identifiers, and change of program layout.